## REMARKS

Reconsideration and allowance are respectfully requested in view of the following remarks. Claims 1, 2, 4, 5, 7-9, 12 and 13 are pending in the present application.

**Claim Rejections Under 35 U.S.C. § 103**

Claims 1, 2, 4, 5, 7-9, 12 and 13 are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over alleged Applicant's Admitted Prior Art (AAPA) (hereinafter, the "Pencil/Paper Method") in view of Miyaguichi (U.S. Patent No. 4,514,592, hereinafter "Miyaguchi"). This rejection is respectfully traversed as follows.

It is asserted in the Office Action that the alleged AAPA of the "Pencil/Paper Method" disclosed in pages 3-5 of the specification corresponds to the claimed features of "repeating step (i) for m-n+1 iterations with the same number and type of operations being performed at each iteration, regardless of the value of the quotient bit obtained, to obtain the quotient q." See Office Action: the paragraph bridging pages 3 and 4. Applicants respectfully disagree.

Page 4 of the specification discloses a division method that can be written in the following manner:

Input: $a=(0, a_{m-1}, \ldots, a_0)$

$b=(b_{n-1}, \ldots, b_0)$

Output: q=a div b and r=a mod b

$A=(0, a_{m-1}, \ldots, a_{m-n+1})$

For j=1 to (m-n+1), do:

$a <- SHL_{m-1}(a, 1); \sigma <-$ carry

$A <- SUB_n(A, b); \sigma < -\sigma$ OR carry

if ($\neg\sigma$ =TRUE) then $A <- ADD_n(A, b)$

if not lsb(a)=1

End for

In the above alleged AAPA of the "Pencil/Paper Method" method, several divisions of an integer A of n+1 bits by the integer b of n bits are successively performed. In this method, according to the value of the quotient bit which is obtained during the current iteration (i.e., the value of σ), an addition ADD n (A, b) is either performed or not. The number of operations performed during an iteration therefore varies according to the result bit obtained during the iteration. As such, the current consumption during each iteration and/or the duration of each iteration varies according to the number of operations performed. By measuring and studying, for example, the trace left by the component when the method is executed, it is possible to determine bit-by-bit the value of the result bits. That is, by an unauthorized review of the trace left behind by the operations, the result bits that might be confidential or secret can be determined. Hence, the "Pencil/Paper Method" method is sensitive, for example, to covert channel attacks.

In contrast, according to Appellants' exemplary embodiments, an integer division is performed for a cryptographic method with the same number and type of operations at each iteration, regardless the value of the bit obtained, so that the method can be secured against covert channel attacks depending on implementation. For example, according to Appellants' exemplary embodiments

described in pages 9 and 10 of the specification, an integer division can be performed with the following steps:

For j = 1 to (m-n+1), do:

$a \leftarrow SHL_{m+1}(a, 1)$ ; $\sigma \leftarrow$ carry

$A \leftarrow (\sigma')SUB_n(A, b) + (\neg\sigma')ADD_n(A, b)$

$\sigma \leftarrow (\sigma' \text{ AND } \sigma') / (\sigma' \text{ AND carry}) / (\sigma' \text{ AND carry})$

lsb(a) $\sigma$

$\sigma' \leftarrow \sigma$

End For

Unlike the "Pencil/Paper Method" method, this sequence of steps does not contain any conditional "If" statements that can affect the number or types of operations performed. For this reason, it is not possible to determine bit-by-bit the value of the result bits by measuring and studying the trace left by the component when the method is executed. As such, the method according to Applicants' exemplary embodiment is not sensitive to covert channel attacks. It is hoped that this explanation will help the Examiner understand why the "Pencil/Paper Method" method does not correspond to the features of "repeating step (i) for m-n+1 iterations with the same number and type of operations being performed at each iteration, regardless of the value of the quotient bit obtained, to obtain the quotient q," as recited in claim 1. These features are clearly not shown in the "Pencil/Paper Method."

Miyaguichi is relied upon as allegedly disclosing performing an integer division performed in a processor. As such, it does not cure the deficiencies of the rejection noted above.

In view of at least the foregoing, it is respectfully submitted that claim 1 is patentable. Claims 2, 4, 5, 7, 8, 9, 12 and 13 are patentable at least because of their dependency from claim 1.

## CONCLUSION

From the foregoing, further and favorable action in the form of a Notice of Allowance is respectfully requested and such action is earnestly solicited.

In the event that there are any questions concerning this amendment, or the application in general, the Examiner is respectfully requested to telephone the undersigned so that prosecution of present application may be expedited.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: May 12, 2011

By: Weiwei Y. Stiltner
Weiwei Y. Stiltner
Registration No. 62979

**Customer No. 21839**
703 836 6620